APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/711,646	09/29/2004	Anatoliy Panasyuk	2006579-0440 (CTX-087)	5645

69665   7590   12/22/2009
CHOATE, HALL & STEWART / CITRIX SYSTEMS, INC.
TWO INTERNATIONAL PLACE
BOSTON, MA 02110

EXAMINER
VOSTAL, ONDREJ C

ART UNIT	PAPER NUMBER
2453	

MAIL DATE	DELIVERY MODE
12/22/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	10/711,646	PANASYUK ET AL.
	Examiner	Art Unit
	O. C. Vostal	2453

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 October 2009*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,8-18 and 20-26* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6, 8-18 and 20-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____.

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   Claims 1-6, 8-18 and 20-26 presented for examination.

2.   Claim 7 and 19 are canceled.

2.   This action is in response to remarks and arguments filed on October 6, 2009,

after RCE non-final rejection of application 10/711646. Application filed on

September 29, 2004.

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described
> as set forth in section 102 of this title, if the differences between the subject matter sought to
> be patented and the prior art are such that the subject matter as a whole would have been
> obvious at the time the invention was made to a person having ordinary skill in the art to which
> said subject matter pertains. Patentability shall not be negatived by the manner in which the
> invention was made.

5.   Claims 1, 2, 13 and 14 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Crump et al., US Patent 2002/ 0,078,208 A1, hereinafter

Crump, in views of Verkama, US Patent Application Publication Number 2001/

0,050,908 A1.

6.   Regarding claim 1, Crump disclose a method for reconnecting a client to a host

service (Crump; [0032]: The examiner considers <u>client connection is re-</u>

<u>established</u> is similar to reconnecting a client to a host service.) the method

comprising:

(a)   providing a first connection between a client and a first protocol service

        executing on a second computing device, and a second connection

        between the first protocol service and a host service executing on a third

        computing device (Crump; fig 4A);

(b)   detecting, by the first protocol service, a disruption in the first connection

        (Crump; [0032]: The examiner considers <u>detects a failure</u> is similar to

        detecting a disruption.);

(c)   re-establishing, by the client, the first connection between the client and

        the first protocol service while maintaining the second connection between

        the first protocol service and the host service (Crump; [0032], [0036] and

        [0039]: The examiner considers <u>client connection is re-established</u> is

        similar to re-establishing the first connection, and considers <u>active X.25</u>

        <u>connections exist</u>… <u>as long as the X.25 network is operative</u> is similar to

        maintaining the second connection.);

Crump do not disclose limitations (d), (e) and (f), but in a similar field of endeavor

Verkama discloses:

(d)   receiving at the first protocol service a ticket associated with the client

        (Verkoma; [0013]: The examiner considers <u>an identifier is allocated to</u> is

        similar to receiving… a ticket, and considers <u>service connection</u> is similar

        to first protocol service.);

(e)   validating, by the first protocol service, the ticket (Verkoma; [0011] and

[0012]: The examiner considers <u>storing an address or an identifier by</u>

<u>which the mobile station can be reached</u> is similar to validating… the

ticket, and considers <u>should be identified everywhere</u> is similar to

validating.); and

(f)   linking, by the first protocol service, after the ticket is validated, the re-

established first connection to the maintained second connection

(Verkama; [0012] and [0013]: The examiner considers <u>MAP protocol</u> is

similar to first protocol service and considers <u>identifier of the service</u>

<u>connection is transferred from the old SSP to the new SSP</u> , <u>by means of</u>

<u>the transferred data, the service connection is established from the new</u>

<u>SSP to the SCP</u> and <u>service connection would have to be re-established</u>

are similar to linking… after the ticket is validated, the re-established first

connection.).

Thus, it would have been obvious to the person of ordinary skill in the art at the

time of the invention to readily recognize the advantage of modifying Crump's

system that provides the user <u>a translating function for recovering multiple</u>

<u>connections in a communications network</u> with the features of Verkama's system

<u>equipment for providing network-initiated information transfer for terminals in a</u>

<u>network.</u>

The motivation being <u>an efficient technique for recovering multiple connections</u> which includes <u>able to communicate with the MS using the PDP address indicated by the intelligent network node</u> and includes continuous connection to/thru network.

7.   Regarding claim 2, Crump do not disclose claim 2, but in a similar field of endeavor Verkama discloses the method of claim 1 wherein step (a) further comprises authenticating the client with the host service during a first communication session between the client and the host service (Verkama; [0029]: The examiner considers <u>authenticating the MS subscriber</u> is similar to authenticating the client.).

Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention to readily recognize the advantage of modifying Crump's system that provides the user <u>a translating function for recovering multiple connections in a communications network</u> with the features of Verkama's system <u>equipment for providing network-initiated information transfer for terminals in a network.</u>

The motivation being <u>an efficient technique for recovering multiple connections</u> which includes <u>able to communicate with the MS using the PDP address</u>

indicated by the intelligent network node and includes continuous connection

to/thru network.

8.   Regarding claim 13, Crump disclose a system for reconnecting a client to a host

service (Crump; [0032]: The examiner considers client connection is re-

established is similar to reconnecting a client to a host service.), the system

comprising:

(a)   a client configured to maintain a first connection with a first protocol

service executing on a second computing device, the client re-establishing

the first connection between the client and the first protocol server while

maintaining the second connection between the first protocol serer and

the host service (Crump; fig 4A, [0032], [0036] and [0039]: The examiner

considers client connection is re-established is similar to re-establishing

the first connection, and considers active X.25 connections exist... as long

as the X.25 network is operative is similar to maintaining the second

connection.);

(b)   the first protocol service configured to maintain the first connection with

the client and a second connection with the host service executing on a

third computing device, the first protocol service:

(ba)   detecting a disruption in the first connection (Crump; [0032]: The

examiner considers detects a failure is similar to detecting a

disruption.),

Crump do not disclose limitations (bb), (bc) and (bd), but in a similar field of

endeavor Verkama discloses:

(bb)   receiving a ticket transmitted by the client and associated with the

client (Verkoma; [0004] and [0013]: The examiner considers

send/receive data packets to/from GPRS MS is similar to

transmitted by the client, considers registering the new MSs and an

identifier is allocated to is similar to a ticket... associated with the

client.);

(bc)   validating the ticket (Verkoma; [0011] and [0012]: The examiner

considers storing an address or an identifier by which the mobile

station can be reached is similar to validating... the ticket, and

considers should be identified everywhere is similar to validating.);

and

(bd)   after the ticket is validated, linking the re-established first

connection to the maintained second connection (Verkama; [0013]:

The examiner considers identifier of the service connection is

transferred from the old SSP to the new SSP , by means of the

transferred data, the service connection is established from the new

SSP to the SCP and service connection would have to be re-

established are similar to linking, by the first protocol server, after

the ticket is validated, the re-established first connection.).

Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention to readily recognize the advantage of modifying Crump's system that provides the user <u>a translating function for recovering multiple connections in a communications network</u> with the features of Verkama's system <u>equipment for providing network-initiated information transfer for terminals in a network.</u>

The motivation being <u>an efficient technique for recovering multiple connections</u> which includes <u>able to communicate with the MS using the PDP address indicated by the intelligent network node</u> and includes continuous connection to/thru network.

9.   Regarding claim 14, Crump do not disclose claim 14, but in a similar field of endeavor Verkama discloses the system of claim 13 wherein the client is authenticated with the host service during a first communication session between the client and the host service (Verkama; [0029]: The examiner considers <u>authenticating the MS subscriber</u> is similar to authenticating the client.).

Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention to readily recognize the advantage of modifying Crump's system that provides the user <u>a translating function for recovering multiple connections in a communications network</u> with the features of Verkama's system

equipment for providing network-initiated information transfer for terminals in a network.

The motivation being an efficient technique for recovering multiple connections which includes able to communicate with the MS using the PDP address indicated by the intelligent network node and includes continuous connection to/thru network.

10.   Claims 3-6, 8-1, 15-18 and 20-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Crump et al., US Patent 2002/ 0,078,208 A1, hereinafter Crump, and in views of Verkama, US Patent Application Publication Number 2001/ 0,050,908 A1, as applied to claim 1 above, and further in views of Laursen et al., US Patent 6,065,120 (effective filing date is December 9, 1997), hereinafter Laursen.

11.   Regarding claim 3, Crump and Verkama do not disclose claim 3, but in a similar field of endeavor Lauren disclose the method of claim 1 wherein step (e) further comprises obtaining, from the ticket, a key and session id (Laursen col 10 lines 63-67 and col 11 lines 1-10; Upon receiving the SR from the client 170, the server 172 creates a server proto session for the client 170 with a session identifier, referred to as session ID. If server 172 is satisfied with the fact that the

client is known, namely Encry[C-nonce, C-nonceModified] in the received SR are successfully decrypted with the shared secret encrypt key, the step on in the client authentication is successful and a correspond session key is generated and stored. SR is similar to ticket.

successfully decrypted with the shared secret encrypt key is similar to obtaining a key.).

Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention to readily recognize the advantage of modifying Crump's and Verkama's system that provides the user a translating function for recovering multiple connections in a communications network with the features of Lauren's system a generic solution for communicating desired ideas or transactions from other devices with rich user interface to such a thin client through a self-provisioned account entry.

The motivation being an efficient technique for recovering multiple connections which includes the user who is the only one who knows the credential information created in an authenticated and secure communication session for the rendezvous, thereby the account becomes truly proprietary and includes securely storing interesting ideas, authentication info and credentials.

12.   Regarding claim 4, Crump and Verkama do not disclose claim 4, but in a similar

field of endeavor Lauren disclose the method of claim 3 wherein step (e) further

comprises using the session id from the ticket to retrieve encrypted

authentication credentials (Laursen col 10 lines 63-67 and col 11 lines 1-10;

Upon receiving the SR from the client 170, the server 172 creates a server proto

session for the client 170 with a session identifier, referred to as session ID. If

server 172 is satisfied with the fact that the client is known, namely Encry[C-

nonce, C-nonceModified] in the received SR are successfully decrypted with the

shard secret encrypt key, the step one in the client authentication is successful

and a correspond session key is generated and stored. SR is similar to ticket. if

server 172 is satisfied... are successfully decrypted... client authentication is

successful is similar to retrieve encrypted authentication credentials.).

Thus, it would have been obvious to the person of ordinary skill in the art at the

time of the invention to readily recognize the advantage of modifying Crump's

and Verkama's system that provides the user a translating function for recovering

multiple connections in a communications network with the features of Lauren's

system a generic solution for communicating desired ideas or transactions from

other devices with rich user interface to such a thin client through a self-

provisioned account entry.

The motivation being <u>an efficient technique for recovering multiple connections</u> which includes <u>the user</u> who <u>is the only one who knows the credential information created in an authenticated and secure communication session for the rendezvous, thereby the account becomes truly proprietary</u> and includes securely storing interesting ideas, authentication info and credentials.

13.   Regarding claim 5, Crump and Verkama do not disclose claim 5, but in a similar field of endeavor Lauren disclose the method of claim 4 wherein step (e) further comprises using the key from the ticket to decrypt the retrieved authentication credentials (Laursen col 11 lines 5-15; <u>successfully decrypted with the shared secret encrypt key, the step one in the client authentication is successful.</u>).

Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention to readily recognize the advantage of modifying Crump's and Verkama's system that provides the user <u>a translating function for recovering multiple connections in a communications network</u> with the features of Lauren's system <u>a generic solution for communicating desired ideas or transactions from other devices with rich user interface to such a thin client through a self-provisioned account entry.</u>

The motivation being <u>an efficient technique for recovering multiple connections</u> which includes <u>the user</u> who <u>is the only one who knows the credential information</u>

created in an authenticated and secure communication session for the

rendezvous, thereby the account becomes truly proprietary and includes securely

storing interesting ideas, authentication info and credentials.

14.   Regarding claim 6, Crump and Verkama do not disclose claim 6, but in a similar

field of endeavor Lauren disclose the method of claim 5 wherein step (e) further

comprises re-authenticating the client with the host service using the decrypted

authentication credentials (Laursen col 11 lines 5-15 and lines 30-35;

successfully decrypted with the shard secret encrypt key, the step one in the

client authentication is successful. If Encry[C-nonce, C-nonceModified] can not

be successfully decrypted due to other reasons such as transmission errors, the

client must reinitiate a new session request to the server in order to establish a

secure communication with the server. Reinitiate.. to establish a secure is

similar to re-authenticate.).

Thus, it would have been obvious to the person of ordinary skill in the art at the

time of the invention to readily recognize the advantage of modifying Crump's

and Verkama's system that provides the user a translating function for recovering

multiple connections in a communications network with the features of Lauren's

system a generic solution for communicating desired ideas or transactions from

other devices with rich user interface to such a thin client through a self-

provisioned account entry.

The motivation being <u>an efficient technique for recovering multiple connections</u> which includes <u>the user</u> who <u>is the only one who knows the credential information created in an authenticated and secure communication session for the rendezvous, thereby the account becomes truly proprietary</u> and includes securely storing interesting ideas, authentication info and credentials.

15.   Regarding claim 8, Crump and Verkama do not disclose claim 8, but in a similar field of endeavor Lauren disclose the method of claim 1 wherein step (f) further comprises generating, after deleting the ticket, a replacement ticket (Laursen col 12 lines 15-20; the client 170 discards the SP 176 and a new session creation may be started over again. <u>new session creation</u> is similar to generating a replacement.).

Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention to readily recognize the advantage of modifying Crump's and Verkama's system that provides the user <u>a translating function for recovering multiple connections in a communications network</u> with the features of Lauren's system <u>a generic solution for communicating desired ideas or transactions from other devices with rich user interface to such a thin client through a self-provisioned account entry.</u>

The motivation being <u>an efficient technique for recovering multiple connections</u> which includes <u>the user</u> who <u>is the only one who knows the credential information created in an authenticated and secure communication session for the rendezvous, thereby the account becomes truly proprietary</u> and includes securely storing interesting ideas, authentication info and credentials.

16.   Regarding claim 9, Crump and Verkama do not disclose claim 9, but in a similar field of endeavor Lauren disclose the method of claim 1 wherein step (a) further comprises generating a ticket at the first protocol service (Lauren col 8 lines 20-26 and col 9 lines 55-65; <u>if supplied usemrname and password match those is the account structure 143, the access requested by the PC 110 is allowed.</u> <u>access requested</u> is similar to receiving. <u>the authentication process is conducted with three message exchanges; a Session Request (SR)…</u> <u>Session Request</u> is similar to ticket. <u>The client 170…</u> <u>initiates a SR 174 to be sent to the server 174.</u> Also, <u>to be sent</u> is similar to generating.).

Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention to readily recognize the advantage of modifying Crump's and Verkama's system that provides the user <u>a translating function for recovering multiple connections in a communications network</u> with the features of Lauren's system <u>a generic solution for communicating desired ideas or transactions from</u>

other devices with rich user interface to such a thin client through a self-

provisioned account entry.

The motivation being an efficient technique for recovering multiple connections

which includes the user who is the only one who knows the credential information

created in an authenticated and secure communication session for the

rendezvous, thereby the account becomes truly proprietary and includes securely

storing interesting ideas, authentication info and credentials.

17.   Regarding claim 10, Crump and Verkama do not disclose claim 10, but in a

similar field of endeavor Lauren disclose the method of claim 9 wherein step (a)

further comprises saving, at the first protocol service, a copy of the ticket

(Laursen col 11 lines 5-7; The information in the received SR is saved in the

server proto-session. Information in the received SR is similar to copy of the

ticket.).

Thus, it would have been obvious to the person of ordinary skill in the art at the

time of the invention to readily recognize the advantage of modifying Crump's

and Verkama's system that provides the user a translating function for recovering

multiple connections in a communications network with the features of Lauren's

system a generic solution for communicating desired ideas or transactions from

other devices with rich user interface to such a thin client through a self-

provisioned account entry.

The motivation being an efficient technique for recovering multiple connections

which includes the user who is the only one who knows the credential information

created in an authenticated and secure communication session for the

rendezvous, thereby the account becomes truly proprietary and includes securely

storing interesting ideas, authentication info and credentials.

18.   Regarding claim 11, Crump and Verkama do not disclose claim 11, but in a

similar field of endeavor Lauren disclose the method of claim **1** wherein step (a)

further comprises transmitting the ticket from the first protocol service to the client

(Laursen col 11 lines 43-47; Right after the successful step one client

authentication, the server 172 responds to the client with a Session reply (SP)

176 to begin a second round authentication; server authentication. Responds to

is similar to transmitting the ticket from.).

Thus, it would have been obvious to the person of ordinary skill in the art at the

time of the invention to readily recognize the advantage of modifying Crump's

and Verkama's system that provides the user a translating function for recovering

multiple connections in a communications network with the features of Lauren's

system a generic solution for communicating desired ideas or transactions from

other devices with rich user interface to such a thin client through a self-

provisioned account entry.

The motivation being an efficient technique for recovering multiple connections

which includes the user who is the only one who knows the credential information

created in an authenticated and secure communication session for the

rendezvous, thereby the account becomes truly proprietary and includes securely

storing interesting ideas, authentication info and credentials.

19.   Regarding claim 15, Crump and Verkama do not disclose claim 15, but in a

similar field of endeavor Lauren disclose the system of claim 13 wherein the

ticket comprises a key and session id (Laursen col 10 lines 63-67; Upon

receiving the SR from the client 170, the server 172 creates a server proto

session for the client 170 with a session identifier, referred to as session ID. If

server 172 is satisfied with the fact that the client is known, namely Encry[C-

nonce, C-nonceModified] in the received SR are successfully decrypted with the

shared secret encrypt key, the step on in the client authentication is successful

and a correspond session key is generated and stored. SR is similar to ticket.

successfully decrypted with the shared secret encrypt key is similar to obtaining a

key.).

Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention to readily recognize the advantage of modifying Crump's and Verkama's system that provides the user <u>a translating function for recovering multiple connections in a communications network</u> with the features of Lauren's system <u>a generic solution for communicating desired ideas or transactions from other devices with rich user interface to such a thin client through a self-provisioned account entry.</u>

The motivation being <u>an efficient technique for recovering multiple connections</u> which includes <u>the user</u> who <u>is the only one who knows the credential information created in an authenticated and secure communication session for the rendezvous, thereby the account becomes truly proprietary</u> and includes securely storing interesting ideas, authentication info and credentials.

20.   Regarding claim 16, Crump and Verkama do not disclose claim 16, but in a similar field of endeavor Lauren disclose the system of claim 15 wherein the ticket is validated by the first protocol service using the session id to retrieve encrypted authentication credentials (Laursen col 10 lines 63-67; <u>Upon receiving the SR from the client 170, the server 172 creates a server proto session for the client 170 with a session identifier, referred to as session ID. If server 172 is satisfied with the fact that the client is known, namely Encry[C-nonce, C-nonceModified] in the received SR are successfully decrypted with the shard</u>

secret encrypt key, the step one in the client authentication is successful and a correspond session key is generated and stored. SR is similar to ticket. if server 172 is satisfied… are successfully decrypted… client authentication is successful is similar to retrieve encrypted authentication credentials.).

Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention to readily recognize the advantage of modifying Crump's and Verkama's system that provides the user a translating function for recovering multiple connections in a communications network with the features of Lauren's system a generic solution for communicating desired ideas or transactions from other devices with rich user interface to such a thin client through a self-provisioned account entry.

The motivation being an efficient technique for recovering multiple connections which includes the user who is the only one who knows the credential information created in an authenticated and secure communication session for the rendezvous, thereby the account becomes truly proprietary and includes securely storing interesting ideas, authentication info and credentials.

21. Regarding claim 17, Crump and Verkama do not disclose claim 17, but in a similar field of endeavor Lauren disclose the system of claim 16 wherein the ticket is further validated by decrypting the retrieved authentication credentials

with the key from the ticket (Laursen col 11 lines 5-15; successfully decrypted with the shared secret encrypt key, the step one in the client authentication is successful.).

Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention to readily recognize the advantage of modifying Crump's and Verkama's system that provides the user a translating function for recovering multiple connections in a communications network with the features of Lauren's system a generic solution for communicating desired ideas or transactions from other devices with rich user interface to such a thin client through a self-provisioned account entry.

The motivation being an efficient technique for recovering multiple connections which includes the user who is the only one who knows the credential information created in an authenticated and secure communication session for the rendezvous, thereby the account becomes truly proprietary and includes securely storing interesting ideas, authentication info and credentials.

22.   Regarding claim 18, Crump and Verkama do not disclose claim 18, but in a similar field of endeavor Lauren disclose the system of claim 17 wherein the client is re-authenticated with the host service using the decrypted authentication credentials (Laursen col 11 lines 5-15 and lines 30-35; successfully decrypted

with the shard secret encrypt key, the step one in the client authentication is successful. If Encry[C-nonce, C-nonceModified] can not be successfully decrypted due to other reasons such as transmission errors, the client must reinitiate a new session request to the server in order to establish a secure communication with the server. Reinitiate.. to establish a secure is similar to re-authenticate.).

Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention to readily recognize the advantage of modifying Crump's and Verkama's system that provides the user a translating function for recovering multiple connections in a communications network with the features of Lauren's system a generic solution for communicating desired ideas or transactions from other devices with rich user interface to such a thin client through a self-provisioned account entry.

The motivation being an efficient technique for recovering multiple connections which includes the user who is the only one who knows the credential information created in an authenticated and secure communication session for the rendezvous, thereby the account becomes truly proprietary and includes securely storing interesting ideas, authentication info and credentials.

23.   Regarding claim 20, Crump and Verkama do not disclose claim 20, but in a

similar field of endeavor Lauren disclose the system of claim 13 wherein the first

protocol service is further configured to generate, after deleting the ticket, a

replacement ticket (Laursen col 12 lines 15-20; the client 170 discards the SP

176 and a new session creation may be started over again. new session

creation is similar to generating a replacement.).

Thus, it would have been obvious to the person of ordinary skill in the art at the

time of the invention to readily recognize the advantage of modifying Crump's

and Verkama's system that provides the user a translating function for recovering

multiple connections in a communications network with the features of Lauren's

system a generic solution for communicating desired ideas or transactions from

other devices with rich user interface to such a thin client through a self-

provisioned account entry.

The motivation being an efficient technique for recovering multiple connections

which includes the user who is the only one who knows the credential information

created in an authenticated and secure communication session for the

rendezvous, thereby the account becomes truly proprietary and includes securely

storing interesting ideas, authentication info and credentials.

24.   Regarding claim 21, Crump and Verkama do not disclose, but in a similar field of

endeavor Lauren disclose the system of claim 13 wherein the first protocol

service is further configured to generate the ticket (Lauren col 8 lines 20-26 and

col 9 lines 55-65; if supplied usemrname and password match those is the

account structure 143, the access requested by the PC 110 is allowed. access

requested is similar to receiving. the authentication process is conducted with

three message exchanges; a Session Request (SR)... Session Request is

similar to ticket. The client 170... initiates a SR 174 to be sent to the server 174.

Also, to be sent is similar to generating.).

Thus, it would have been obvious to the person of ordinary skill in the art at the

time of the invention to readily recognize the advantage of modifying Crump's

and Verkama's system that provides the user a translating function for recovering

multiple connections in a communications network with the features of Lauren's

system a generic solution for communicating desired ideas or transactions from

other devices with rich user interface to such a thin client through a self-

provisioned account entry.

The motivation being an efficient technique for recovering multiple connections

which includes the user who is the only one who knows the credential information

created in an authenticated and secure communication session for the

rendezvous, thereby the account becomes truly proprietary and includes securely

storing interesting ideas, authentication info and credentials.

25.   Regarding claim 22, Crump and Verkama do not disclose claim 22, but in a

similar field of endeavor Lauren disclose the system of claim 12 wherein the first

protocol service is further configured to save a copy of the ticket (Laursen col 11

lines 5-7; The information in the received SR is saved in the server proto-

session. Information in the received SR is similar to copy of the ticket.).

Thus, it would have been obvious to the person of ordinary skill in the art at the

time of the invention to readily recognize the advantage of modifying Crump's

and Verkama's system that provides the user a translating function for recovering

multiple connections in a communications network with the features of Lauren's

system a generic solution for communicating desired ideas or transactions from

other devices with rich user interface to such a thin client through a self-

provisioned account entry.

The motivation being an efficient technique for recovering multiple connections

which includes the user who is the only one who knows the credential information

created in an authenticated and secure communication session for the

rendezvous, thereby the account becomes truly proprietary and includes securely

storing interesting ideas, authentication info and credentials.

26.   Regarding claim 23, Crump and Verkama do not disclose claim 23, but in a

similar field of endeavor Lauren disclose the system of claim 13 wherein the first

protocol service is further configured to transmit the ticket to the client (Laursen

col 11 lines 43-47; Right after the successful step one client authentication, the

server 172 responds to the client with a Session reply (SP) 176 to begin a

second round authentication; server authentication. Responds to is similar to

transmitting the ticket from.).

Thus, it would have been obvious to the person of ordinary skill in the art at the

time of the invention to readily recognize the advantage of modifying Crump's

and Verkama's system that provides the user a translating function for recovering

multiple connections in a communications network with the features of Lauren's

system a generic solution for communicating desired ideas or transactions from

other devices with rich user interface to such a thin client through a self-

provisioned account entry.

The motivation being an efficient technique for recovering multiple connections

which includes the user who is the only one who knows the credential information

created in an authenticated and secure communication session for the

rendezvous, thereby the account becomes truly proprietary and includes securely

storing interesting ideas, authentication info and credentials.

27.   Claims 12 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable

        over Crump et al., US Patent 2002/ 0,078,208 A1, hereinafter Crump, and in

        views of Verkama, US Patent Application Publication Number 2001/ 0,050,908

        A1, as applied to claims 1 and 13 above, and further in views of Yamanaka et al.,

        US Patent 6,757,283 B1, hereinafter Yamanaka.

28.   Regarding claim 12, Crump and Verkama do not disclose claim 12, but in a

        similar field of endeavor Yamanaka disclose

        the method of claim 1 wherein step (a) further comprises deleting the ticket

        automatically after a pre-determined period of time (Yamanaka; col 3 lines 40-53:

        The examiner considers <u>identifier</u> is similar to ticket, and considers <u>at a</u>

        <u>predetermined time</u> is similar to a pre-determined period of time.).

        Thus, it would have been obvious to the person of ordinary skill in the art at the

        time of the invention to readily recognize the advantage of modifying Crump's

        and Verkama's system that provides the user <u>a translating function for recovering</u>

        <u>multiple connections in a communications network</u> with the features of

        Yamanaka's system <u>adds to a packet a content identifier for identifying the</u>

        <u>content.</u>

The motivation being <u>an efficient technique for recovering multiple connections</u> which includes <u>a push network capable of making effective use of the memory resources in each node</u> and includes cleaning unnecessary information.

29.   Regarding claim 24, Crump and Verkama do not disclose claim 24, but in a similar field of endeavor Yamanaka disclose the system of claim 13 wherein the first protocol service is further configured to automatically delete the ticket after a pre-determined period of time (Yamanaka; col 3 lines 40-53: The examiner considers <u>identifier</u> is similar to ticket, and considers <u>at a predetermined time</u> is similar to a pre-determined period of time.).

Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention to readily recognize the advantage of modifying Crump's and Verkama's system that provides the user <u>a translating function for recovering multiple connections in a communications network</u> with the features of Yamanaka's system <u>adds to a packet a content identifier for identifying the content.</u>

The motivation being <u>an efficient technique for recovering multiple connections</u> which includes <u>a push network capable of making effective use of the memory resources in each node</u> and includes cleaning unnecessary information.

30.   Claims 25 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Crump et al., US Patent 2002/ 0,078,208 A1, hereinafter Crump, and in

views of Verkama, US Patent Application Publication Number 2001/ 0,050,908

A1, as applied to claims 1 and 13 above, and further in views of Mirashrafi et al.,

US Patent Number 6,304,637 B1, hereinafter Mirashrafi.

31.   Regarding claim 25, Crump and Verkama do not disclose claim 25, but in a

similar field of endeavor Mirashrafi disclose the method of claim 1, wherein the

third computing device is the second computing device (Mirashrafi; col 14 lines

57-67: The examiner considers page Bridgeport is similar to third computing

device and considers changeover Bridgeport is similar to a second computing

device. a member bridgeport actually can be a page bridgeport and a

changover bridgeport at the same time for either same or different clients.).

Thus, it would have been obvious to the person of ordinary skill in the art at the

time of the invention to readily recognize the advantage of modifying Crump's

and Verkama's system that provides the user a translating function for recovering

multiple connections in a communications network with the features of

Mirashrafi's system apparatus for establishing and facilitating a direct quality

voice call to a telephone handset on behalf of a client computer.

The motivation being <u>an efficient technique for recovering multiple connections</u> which includes <u>the ability of the network to successfully transmit information from one point in the network to another determines the quality of the network</u> and includes reusing equipment at different locations.

32.   Regarding claim 26, Crump and Verkama do not disclose, but in a similar field of endeavor Mirashrafi disclose the system of claim 13, wherein the third computing device is the second computing device (Mirashrafi; col 14 lines 57-67: The examiner considers <u>page Bridgeport</u> is similar to third computing device and considers <u>changeover Bridgeport</u> is similar to a second computing device. <u>a member bridgeport actually can be a page bridgeport and a changover bridgeport at the same time for either same or different clients</u>.).

Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention to readily recognize the advantage of modifying Crump's and Verkama's system that provides the user <u>a translating function for recovering multiple connections in a communications network</u> with the features of Mirashrafi's system <u>apparatus for establishing and facilitating a direct quality voice call to a telephone handset on behalf of a client computer.</u>

The motivation being <u>an efficient technique for recovering multiple connections</u> which includes <u>the ability of the network to successfully transmit information from</u>

one point in the network to another determines the quality of the network and
includes reusing equipment at different locations.

Response to Arguments

33.   Applicant's arguments filed October 6, 2009, stated neither Mirshrfi, Crump,
Jones nor Laursen teaches or suggests each and every element of the claimed
invention because non of these references teaches or suggests linking after a
ticket is validated, a re-established first connection to a maintained second
connection between a first protocol service and a host service as required by
independent claims 1 and 13.

Examiner's response is after reviewing X.25 protocol, a combination of Crump
and Verkama do disclose linking after a ticket is validated, a re-established first
connection to a maintained second connection between a first protocol service
and a host service. For an explanation of validating, please refer to [0008] of the
original specification. For an explanation of temporary disruption in a network
connection and maintaining second connection, please refer to [0006] of the
original specification. Original specification discloses that temporary disruption
occurs when roaming (transferring as disclosed by Verkama in an X.25 protocol
area.) between different access points. Refer to 103 rejection above.
Application original specification supports rejection. A X.25 protocol specification
(about 1995 vintage) can be obtained, if necessary.

Conclusion

34.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure. Applicant is reminded that in amending in response to a

rejection of claims, the patentable novelty must be clearly shown in view of the

state of the art disclosed by the references cited and the objection made.

Applicant must show how the amendments avoid such references and

objections. See 37 CFR 1.111(c).

35.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to O. Charlie Vostal whose telephone number is

571-270-3992. The examiner can normally be reached on 7:30am to 5:00pm

EST Monday thru Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Joseph Thomas can be reached on 571-272-6776. The fax phone

number for the organization where this application or proceeding is assigned is

571-270-4992.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR

only. For more information about the PAIR system, see http://pair-

direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-

free). If you would like assistance from a USPTO Customer Service

Representative or access to the automated information system, call 800-786-

9199 (IN USA OR CANADA) or 571-272-1000.

/O. C. Vostal/
Examiner
Art unit 2453
December 16, 2009

/Liangche A. Wang/
Primary Examiner, Art Unit 2453